AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

initializing a pseudo-random number generator (PRNG);

obtaining local seeding information from a host;

securely obtaining additional seeding information from one or more remote entropy servers using a secure entropy collection protocol, wherein the securely obtaining of the additional seeding information is repeated for each entropy server, wherein the secure entropy collection protocol is to perform:

generating a key pair including a temporary asymmetric public key and a temporary asymmetric private key,

encrypting the temporary public key with a public key associated with a remote entropy server,

decrypting the temporary public key with a private key associated with the remote entropy server,

encrypting the additional seeding information with the temporary public key, and

decrypting the additional seeding information with the temporary private key; and

stirring the PRNG ~~with~~ via the local seeding information and the additional seeding information.

2. (Previously Presented) The method of claim 1, wherein the initializing of the PRNG comprises initializing an internal state of the PRNG with a random value.

3. (Previously Presented) The method of claim 2, wherein the random value comprises a seed.

4. (Cancelled)

5. (Previously Presented) The method of claim 1, wherein the one or more remote entropy servers maintain random state pool to supply the host with the random value.

6. (Previously Presented) The method of claim 1, wherein the securely obtaining of the seeding information from the one or more remote entropy servers includes using a privacy protocol.

7. (Original) The method of claim 6, wherein the privacy protocol comprises secure sockets layer (SSL) protocol.

8. (Original) The method of claim 6, wherein the privacy protocol comprises transport layer security (TLS) protocol.

9. (Previously Presented) The method of claim 1, wherein the stirring of the PRNG comprises producing a cryptographically random stream of bits.

Claims 10-16 (Cancelled)

17. (Currently Amended) An entropy enhancing system comprising:

a local system including a host and a pseudo-random number generator (PRNG), the local system to

initialize the PRNG by obtaining local seeding information from the host,

securely obtain additional seeding information from one or more remote entropy servers using a secure entropy collection protocol, wherein the securely obtaining of the additional seeding information is

repeated for each entropy server, the secure entropy collection protocol is to perform:

generating a key pair including a temporary asymmetric public key and a temporary asymmetric private key,

encrypting the temporary public key with a public key associated with a remote entropy server,

decrypting the temporary public key with a private key associated with the remote entropy server,

encrypting the additional seeding information with the temporary public key, and

decrypting the additional seeding information with the temporary private key; and

stir the PRNG ~~with~~ via the local seeding information and the additional seeding information.

18. (Previously Presented) The entropy enhancing system of claim 17, wherein the local system generates the local seeding information at the host.

19. (Previously Presented) The entropy enhancing system of claim 17, wherein the one or more remote systems generates the remote seeding information at the one or more entropy servers.

20. (Previously Presented) The entropy enhancing system of claim 17, wherein the entropy servers comprise one or more of the following: hardware and software.

Claims 21-24 (Cancelled)

25. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

initialize a pseudo-random number generator (PRNG);

obtain local seeding information from a host;

securely obtain additional seeding information from one or more remote entropy servers using a secure entropy collection protocol, wherein the securely obtaining of the additional seeding information is repeated for each entropy server, wherein the secure entropy collection protocol is to:

generate a key pair including a temporary asymmetric public key and a temporary asymmetric private key,

encrypt the temporary public key with a public key associated with a remote entropy server,

decrypt the temporary public key with a private key associated with the remote entropy server,

encrypt the additional seeding information with the temporary public key, and

decrypt the additional seeding information with the temporary private key; and

stir the PRNG ~~with~~ via the local seeding information and the additional seeding information.

26. (Previously Presented) The machine-readable medium of claim 25, wherein the initializing of the PRNG comprises initializing an internal state of the PRNG with a random value.

27. (Previously Presented) The machine-readable medium of claim 26, wherein the random value comprises a seed.

28. (Cancelled)

29. (Previously Presented) The machine-readable medium of claim 25, wherein the one or more remote entropy servers maintain random state pool to supply the host with the random value.

30. (Previously Presented) The machine-readable medium of claim 25, wherein the stirring of the PRNG comprises producing a cryptographically random stream of bits.